

1086-11-713

Ken McMurdy* (kcmurdy@ramapo.edu), Department of Mathematics (TAS), Ramapo College of New Jersey, 505 Ramapo Valley Rd., Mahwah, NJ 07430. *A New Algorithm for Computing Endomorphism Rings of Supersingular Elliptic Curves.*

It is well known from the work of M. Deuring that there is a one-to-one correspondence between endomorphism rings of supersingular elliptic curves mod p and the maximal orders in the quaternion algebra $\mathbb{Q}_{p,\infty}$ to which they are isomorphic. Most algorithms for making the isomorphisms or even the correspondence explicit, however, inevitably involve some “blind searching” on either the quaternion side, the elliptic curve side, or both. Here we describe an algorithm which is relatively easy to implement and contains almost no searching. The key idea is to apply W. Waterhouse’s theory of kernel ideals, as developed in his Harvard thesis. (Received September 11, 2012)